INSIGHT ENGINES

Data Sheet

Empowering people to easily ask questions of their machine data
*Focus on insights and outcomes*

# INSIGHT INVESTIGATOR FOR SPLUNK

## The Challenge

Many cybersecurity teams use Splunk to better detect, investigate, and visualize threats. The challenge they face is a combination of skills shortage and the time / effort / expertise required to create complex queries to access their machine data. Recognizing that the Splunk Search Processing Language (SPL) is designed for advanced queries and experts, cybersecurity leaders know they need a different way to arm entry-level analysts to query Splunk and investigate and empower Splunk experts to concentrate on threat hunting.

## The Solution

Insight Investigator for Splunk enables people to easily ask questions of their machine data. Powered by Insight Engines' unique Natural Language Processing (NLP) technology, Insight Investigator allows analysts to type in plain English, (not complex SPL query language), the inquiries they want to pursue. Insight Investigator is an App that installs on Splunk Enterprise and delivers immediate benefits. Entry-level analysts can quickly add value by investigating and mitigating threats. Senior cybersecurity analysts can focus on advanced work. They can even use the translated SPL queries from Insight Investigator to improve incident response rates and accelerate complex query development. Insight Investigator is optimized for cybersecurity, understanding the language, use cases and queries.

**Insight Engines Query**

```
"Show me vulnerable systems
 with failed updates"
```

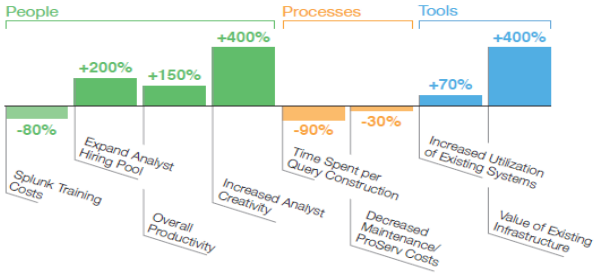
**SPL Query**

Search to show what vulnerable systems had failed updates

```
| tstats allow_old_summaries=t append=t
prestats=t summariesonly=t count values(Up-
dates.severity) as Updates.severity from
datamodel=Updates where Updates.status="-
failure" earliest=06/20/2016:00:00:00
latest=06/27/2016:00:00:00 by Updates.
dest, Updates.signature
| tstats allow_old_summaries=t append=t
prestats=t summariesonly=t count from
datamodel=Vulnerabilities where earliest
=06/20/2016:00:00:00 latest=06/27/2016:
00:00:00 by Vulnerabilities.dest
| fillnull value="" Updates.signature
| eval dest=coalesce('Updates.dest',
'Vulnerabilities.dest'), join_node=if
(isnotnull('Updates.dest'),"Updates",
"Vulnerabilities")
| stats count values(Updates.severity) as
Updates.severity by dest, join_node,
Updates.signature
| eval count_Updates=if(join_node==
"Updates", 'count', null()), count_ Vulner-
abilities=if(join_node=="Vulnerabilities",
'count', null())
| stats list(count_Updates) as count_
Updates list(Updates.signature) as
Updates.signature list(count_Vulnerabili-
ties) as count_Vulnerabilities values(Up-
dates.severity) as Updates.severity by dest
| where isnotnull('count_Updates') AND
isnotnull('count_Vulnerabilities')
| stats sum(count) as count
```

## Natural Language Processing

Insight Engines' patented NLP search technology is much more than keyword lookups from a dictionary. It is a real-time parser that examines the search query to understand meaning, intent and context. In seconds, it produces highly-efficient SPL queries, accurate results, and powerful visualizations.




## Strong ROI

Clients have achieved quantifiable benefits and impact. Accurate queries and visual results in minutes versus hours. $1M in cost reductions. ROI in months.

## Benefits of Insight Investigator for Splunk

**Unlock the Full Value of Splunk**
On average, only 1% of machine data is used. Access and realize the benefits.

**Strengthen Security Posture**
Discover, investigate, and mitigate cyberthreats faster.

**Democratize your Data**
Empower anyone to garner insights from machine data.

**Improve Productivity**
Analyst time is spent defeating threats, not writing queries.

**Less Reliance on SPL Experts**
Up-level your workforce, hire and train entry-level analysts.

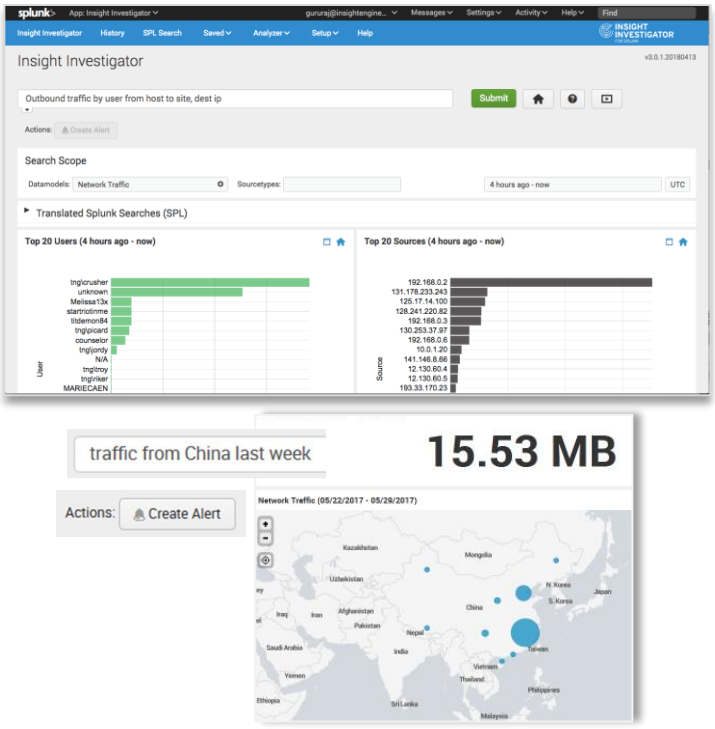
**Faster Incident Response**
Plain English queries are automatically translated into highly efficient SPL, resulting in faster searches and improved response time.

## Returns Rich Results Fast

Enter a plain English search and Insight Investigator automatically, in real-time, handles the SPL translation and presents rich visualizations and insights. Searches can leverage multiple data sources.

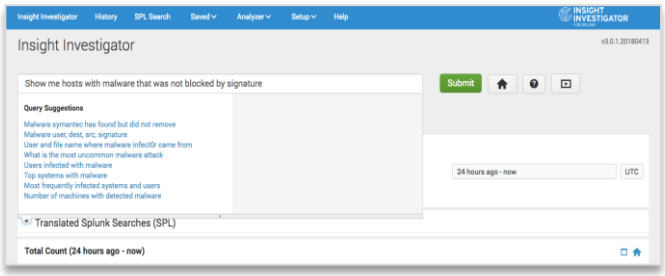
## Reports, Visualizations, Alerts

Insight Investigator dynamically visualizes search results in context by understanding the query and delivering actionable insights. For example, in the image on the right, Insight Investigator understands the search centers around location and shows a geo-IP map. Users can also easily turn a plain English query into an alert.

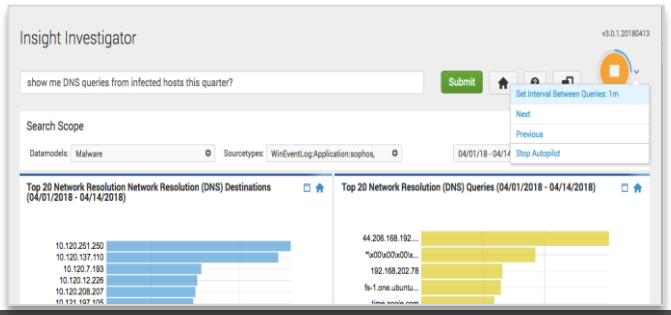



## Query Recommendations & AutoPilot

Insight Investigator offers rich capabilities to augment human intelligence with comprehensive and relevant query suggestions via the query recommendations engine.




AutoPilot auto-asks interesting questions at regular intervals to uncovers new issues. It is dynamic, replacing static dashboards and surfacing anomalies quickly. It automatically generates thousands of queries every day.




## Use the Raw Splunk SPL

Analysts of all levels can benefit from the SPL generated by Insight Investigator: learn SPL, use it as a shortcut to create complex queries, quickly check the accuracy of SPL queries.


## Technical and Installation Details

- 100% self-contained Splunk App
- Can install in minutes
- No additional hardware required
- Installs on a search head or search head cluster
- Requires only Splunk Enterprise
- Leverages Splunk Common Information Model (CIM)
- Will run in any environment Splunk Enterprise is running in

## ABOUT INSIGHT ENGINES

Insight Engines was founded with the mission to empower humans to garner insights from their machine data, and thereby inspiring and fostering an intuitive organization. With its patented natural language processing (NLP) technology, Insight Engines enables people to easily ask questions from complex data. The company's products unlock the value of machine data by making it accessible and actionable to anyone in an organization.

**www.insightengines.com**